CLAIM AMENDMENTS

Claim Amendment Summary

Claims pending

- Before this Amendment: Claims 1-5, 8-17 and 19-32
- After this Amendment: Claims 1-5, 8-17 and 19-32

Non-Elected, Canceled, or Withdrawn claims: None

Amended claims: 1, 10, 14, and 22-28

New claims: None

Claims:

1. (Currently Amended) A method comprising:

receiving an event from a first security engine;

identifying a second security engine configured to utilize information contained in the event, wherein the second security engine is unaware of the first security engine; and

communicating the information contained in the event to the second security engine via an event manager, wherein the event corresponds to identifying a password that does not comply with predetermined criteria; and

with the first security engine, the second security engine, and the event manager being included in a single host computer.

2. (Previously Presented) A method as recited in claim 1 wherein the event identifies a password that does not comply with a length criteria.

3. (Previously Presented) A method as recited in claim 1 wherein the event identifies an action performed by the first security engine in response to a detected vulnerability.

4. (Original) A method as recited in claim 1 wherein the first security engine and the second security engine are application programs.

5. (Previously Presented) A method as recited in claim 1 wherein the event identifies a password that does not include one or more required characters.

6-7. (Cancelled).

8. (Original) A method as recited in claim 1 wherein the first security engine is a vulnerability analysis application program.

9. (Original) A method as recited in claim 1 further comprising:

identifying a third security engine configured to utilize information contained in the event; and

communicating the information contained in the event to the third security engine.

10. (Currently Amended) A method as recited in claim 1 further comprising:

receiving an updated security policy;

identifying at least one security engine that previously requested the security policy ~~associated with the updated security policy~~; and

providing the updated security policy to the identified security engine.

11. (Original) A method as recited in claim 1 further comprising:

receiving a request for data from the first security engine; and

communicating the requested data to the first security engine.

12. (Original) A method as recited in claim 1 further comprising storing information contained in the event in a central location accessible to a plurality of security engines.

13. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 1.

14. (Currently Amended) A method comprising:

receiving a security-related event from a first security-related application program, the security-related event being associated with a system state;

identifying information contained in the security-related event;

identifying a second security-related application program associated with the information contained in the security-related event, wherein the second security-related application program is unaware of the first security-related application program; ~~and~~

communicating the information contained in the security-related event to the second security-related application program via an event manager; and

with the first security-related application program, the second security-related application program, and the event manager being included in a single host computer.

15. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a network connection is wired or wireless.

16. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a host computer is accessing a corporate network.

17. (Previously Presented) A method as recited in claim 14 wherein the information includes whether a host computer is accessing an unknown network.

18. (Cancelled).

19. (Original) A method as recited in claim 14 further comprising:

receiving system state information from a third security-related application program; and

storing the system state information such that the system state information is accessible to the first security-related application program and the second security-related application program.

20. (Original) A method as recited in claim 14 further comprising:

identifying a third security-related application program associated with the information contained in the security-related event; and

communicating the information contained in the security-related event to the third security-related application program.

21. (Original) One or more computer-readable memories containing a computer program that is executable by a processor to perform the method recited in claim 14.

22. (Currently Amended) One or more tangible computer-readable media having stored thereon a computer program executed by one or more processors, comprising:

a first security engine associated with a first type of security attack, the first security engine including configuration to detect a password that does not comply with predetermined criteria;

a second security engine associated with a second type of security attack, wherein the second security engine is unaware of the first security engine; ~~and~~

an event manager coupled to receive events from the first security engine and the second security engine, the event manager further to identify information contained in the events and to identify at least one security engine associated with information contained in a particular event, and further to communicate the information contained in the particular event to the at least one security engine; and

with the first security engine, the second security engine, and the event manager being included in a single host computer.

23. (Currently Amended) ~~A system~~ One or more tangible computer-readable media as recited in claim 22 wherein the information contained in the events identifies a type of security attack.

24. (Currently Amended) ~~A system~~ One or more tangible computer-readable media as recited in claim 22 wherein the information contained in each event identifies an action taken in response to a security attack.

25. (Currently Amended) ~~A system~~ One or more tangible computer-readable media as recited in claim 22 wherein the information contained in the events includes system state information.

26. (Currently Amended) ~~A system~~ One or more tangible computer-readable media as recited in claim 22 further comprising a third security engine coupled to the event manager and associated with a third type of security attack.

27. (Currently Amended) ~~A system~~ One or more tangible computer-readable media as recited in claim 22 further comprising a storage device coupled to the event manager, the first security engine and the second security engine, the storage device to store event information.

28. (Currently Amended) One or more tangible computer-readable media having stored thereon a computer program that, when executed by one or more processors, causes the one or more processors to:

receive a first security-related event from a first service, the first security-related event corresponding to a network-related aspect of a system state;

identify information contained in the first security-related event;

receive a second security-related event from a second service, wherein the second service is unaware of the first service;

identify information contained in the second security-related event;

communicate information contained in the first security-related event to the second service via an event manager; ~~and~~

communicate information contained in the second security-related event to the first service via the event manager; and

with the first service, the second service, and the event manager being included in a single host computer.

29. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the first security-related event identifies a particular type of security attack.

30. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the one or more processors further store the information contained in the first security-related event and the information contained in the second security-related event for access by other services.

31. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the one or more processors further communicate information contained in the first security-related event to a third service.

32. (Previously Presented) One or more tangible computer-readable media as recited in claim 28 wherein the first service is associated with a first type of security attack and the second service is associated with a second type of security attack.